REMARKS

In response to the Office Action dated January 2, 2004, Applicant respectfully requests reconsideration and withdrawal of the objection and rejections of the claims.

The Office Action states that claims 4-6 are objected to as being in improper form, since a multiple dependent claim cannot depend from another multiple dependent claim. Applicant notes, however, that the multiple dependency of the claims was removed in a Preliminary Amendment filed concurrently with the national phase application papers on September 10, 2001. The Examiner is respectfully requested to confirm that the Preliminary Amendment has been entered, and to consider claims 4-6 on their merits in his further review of the claims. If the Preliminary Amendment cannot be located, kindly contact Applicant's undersigned representative at the number listed below, and a duplicate copy will be immediately supplied.

Claims 1-3 and 7 were rejected under 35 U.S.C. § 102, on the grounds that they were considered to be anticipated by the Moreau patent, U.S. Patent No. 6,069,954. In addition, claim 8 was rejected under 35 U.S.C. § 103, on the grounds that it was considered to be unpatentable over the Moreau patent. It is respectfully submitted, however, that the Moreau patent neither anticipates, nor otherwise suggests, the subject matter set forth in the pending claims.

As discussed in detail in the introductory portion of the specification, the present invention is directed to countermeasures against attacks on the integrity of a secret key cryptographic algorithm, using differential power analysis (DPA). The invention is particularly concerned with secret key cryptographic algorithms that

employ a number of successive calculation cycles, in which first data is applied at the input of the first cycle, and final data is derived at the output of the last cycle. An example of such a cryptographic algorithm is the Data Encryption Standard (DES) algorithm depicted in Figures 3 and 4 of the application. Referring thereto, the first data comprises a binary word e, which is divided into two input parameters L0 and R0. The successive calculation cycles of the algorithm are labeled T1...T16. Within each cycle, a calculation means is utilized to supply an output data item from an input data item. In the illustrated example, this calculation means is denoted by the operation SBOX. Referring to Figures 5 and 6, this operation is implemented with lookup table $TC_0$1...$TC_0$8. Each calculation means receives a 6-bit input word E=b1...b6, and produces a 4-bit output word S=a1...a4. It can be seen that this same sequence of operations is carried out in each of the 16 stages of the algorithm. The outputs of the final stage, L16 and R16, are concatenated to produce the final data that constitutes the encrypted message.

As a countermeasure to DPA attacks, the present invention employs two modifications to the conventional algorithm. One of these modifications is to apply random values to the input data item and to the output data item of the calculation means. In the context of the application, the first random value is labeled u and the second random value is labeled v. A second calculation means TC_M is derived from the stored lookup tables TC_0 by applying the random values to the input data E and the output data S, respectively. See, for example, the translation of the Annex to the International Preliminary Examination Report, at page 22, lines 13-26.

The second modification provided by the present invention is to apply the second random value to the first input data by means of an EXCLUSIVE OR

operation. Referring to Figure 9, it can be seen that the input data L0, R0 first undergoes an EXCLUSIVE OR operation with the random value v. The randomness provided by this operation is maintained through the sixteen calculation cycles of the algorithm. To derive the final encrypted data, the output values from the 16^{th} stage undergo an EXCLUSIVE OR operation with the random value v, to produce the conventional outputs L16, R16.

The rejection of the claims states that the Moreau patent discloses a cryptography algorithm which includes two successive pseudo-random and pseudo independent encryption steps. It is respectfully submitted, however, that the disclosure of the Moreau patent does not suggest the claimed subject matter. Referring to Figure 1, it can be seen that a bit of clear text, m_i, first undergoes an EXCLUSIVE OR operation with a random value $k2_i$. The result of this operation then undergoes another EXCLUSIVE OR with a second random value $k1_i$ to produce a bit of cipher text e_i. The mere fact that the Moreau patent discloses the use of two randomly generated bits, as well as two EXCLUSIVE OR operations, is not sufficient to anticipate the claimed subject matter. For instance, claim 1 recites that at least one random value is applied to the input data item and to the output data item of the calculation means that is performed in each calculation cycle. The Office Action has not identified any structure or operation in the Moreau patent that corresponds to such a calculation means. More importantly, even if such a calculation means is present, the Office Action does not indicate where the patent teaches that a random value is applied to *both* an input data item and an output data item of such a calculation means. For at least these reasons, therefore, the subject matter of claim 1 and its dependent claims is not anticipated.

As a further distinction, claim 2 recites the step of using an EXCLUSIVE OR operation to apply the second random value to the final data supplied by the last cycle of the algorithm. The Office Action does not indicate where this subject matter can be found in the teachings of the Moreau patent.

Claim 3 recites that, at the end of *each* cycle, an additional operation is executed to eliminate the first random value at the output of that cycle. For instance, in the example of Figure 9, the EXCLUSIVE OR operation CP(p(u)) is performed at the end of each cycle. Again, it is not apparent how the Moreau patent can be interpreted to anticipate, or otherwise suggest, this claimed subject matter.

Claim 7 recites an electronic security component that has a first calculation means stored in memory, e.g., TC_0, and a second calculation means that is calculated at each new execution of the algorithm, e.g., TC_M, by applying random numbers to the input and output data items of the first calculation means. Again, it is respectfully submitted that the mere fact that the Moreau patent discloses two EXCLUSIVE OR operations with two random values does not anticipate the claimed subject matter. The Office Action does not indicate how the Moreau patent is being interpreted to disclose a calculation means, much less the calculation of a new calculation means, using two random values, each time the algorithm is executed.

Claims 1, 3, 5 and 7 have been amended to remove a possible unintended interpretation of these claims, and otherwise improve their readability. These amendments are not being made for the purpose of overcoming the rejection, since the distinguishing features identified above were recited in the claims prior to the amendments.

In view of the foregoing, it is respectfully submitted that the pending claims are neither anticipated, nor otherwise suggested, by the Moreau patent. Reconsideration and withdrawal of the rejections are therefore respectfully requested.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

Date: June 2, 2004

By: _____
James A. LaBarre
Registration No. 28,632

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620
88132_1.DOC